Microsoft 基準安全分析器 (MBSA) 1.0 版問答

2001 年 4 月 22 日

問：MBSA V1 支援什麼作業系統？

答： MBSA 可以安裝並運行在 Microsoft® Windows® 2000 Server、Windows 2000 專業版、Windows XP Home Edition 和 Windows XP Professional 上。該工具可以在網路上針對 Microsoft Windows NT® 4.0 Server 和 Windows NT 4.0 Workstation、Windows 2000 Server、Windows 2000 Workstation 和 Windows XP Professional 及 Home Edition 系統運行。MBSA 不在 Windows 95、98 或 Me 系統上運行。注 - 1.0 版 (V1) 尚未正式支援 Windows .Net Server。

問：MBSA 可掃描哪些應用程式/程式？

答： MBSA V1 掃描 Windows NT 4.0、Windows 2000、Windows XP、Microsoft Internet Information Services 4.0 和 5.0、Microsoft Internet Explorer 5.01 及更高、Microsoft SQL Server 7.0、SQL Server 2000、Microsoft Office 2000 以及 Microsoft Office XP。

問：MBSA 是否取代了 Microsoft Personal Security Advisor (MPSA)？

答： 是的，MBSA 取代了 MPSA。MBSA 是 Microsoft Personal Security Advisor (MPSA) 工具的一個超集合，因爲它包括了 MPSA 中的所有檢查功能。MBSA 還可以執行其他一些應用程式檢查（如 IIS、SQL），並且對伺服器和工作站都可以掃描，而且既可本地掃描，也可通過網路遠端掃描。

問：MBSA 安全報告存放在什麼位置？

答：安全報告的默認存儲位置是 %userprofile%\SecurityScans。

問：MBSA V1 支援什麼語言？

答： MBSA V1 現在只有英文版。不過，它能夠遠端掃描許多本地化的產品。MBSA 未來的版本將本地化爲其他一些語言。

問：MBSA 如何與 HFNetChk 配合使用？

答： MBSA 使用 HFNetChk 來掃描 Windows、IIS 和 SQL Server 中缺少的即時修補程式和 service pack。HFNetChk 通過引用一個可擴展標記語言 (XML) 安全即時修補程式資料庫來完成此項工作，該資料庫由 Microsoft 不斷地更新。由 HFNetChk 使用，並因而也由 MBSA 使用的這個 XML 資料庫，包含了關於每種 Microsoft 產品各有哪些即時修補程式的資訊。此文件包含安全公告的名稱和標題，關於針對具體產品的安全即時修補程式的詳細資料，其中包括：每個即時修補程式套裝軟體中的文件和它們的文件版本，即時修補程式安裝套裝軟體應用的校驗和、註冊表項，關於哪些修補程式可取代哪些其他修補程式的資訊，以及相關的 Microsoft 知識庫文章編號等。在 MBSA 發行後，HFNetChk 仍將作爲 Microsoft 安全網站上一項可獨立下載的內容提供。

問：MBSA 與 HFNetChk 相比有哪些優勢？

答：MBSA 是 HFNetChk 的功能的一個超集合。HFNetChk 僅僅能夠處理即時修補程式和 Service Pack，而 MBSA 則提供了一個易用的介面和更多的功能。這些

功能包括：檢查 Windows 桌面和伺服器是否採用了安全方面的常用最佳做法，比如強密碼；掃描運行 IIS 和 SQL Server 的伺服器，以查找安全方面的常見配置錯誤；檢查 Microsoft Office、Outlook 和 Internet Explorer 中是否存在未恰當配置的安全區域設置。Microsoft 建議客戶利用 MBSA 工具，因爲其功能既加強了 HFNetChk 工具原有的功能，同時還向客戶提供了 HFNetChk 工具本身無法提供的其他功能和最佳做法。

問：如果我的代理伺服器要求身份驗證，那麼怎樣才能下載必需的文件來運行掃描？

答： 您可以從以下 Microsoft Web 站點下載用來進行即時修補程式檢查的、經簽名的 mssecure.XML 文件：http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab。您還可以訪問以下 Microsoft Web 站點上未壓縮的 XML 文件：http://www.microsoft.com/technet/security/search/mssecure.xml。請將 XML 和 CAB 文件都放在 MBSA 的安裝文件夾中。

問：爲什麼 MBSA 不告訴我關於 MS02-018 和其他 IIS 即時修補程式的資訊？

答： MBSA 將缺少的特定於 IIS 的即時修補程式顯示在生成的掃描報告中的 IIS Vulnerabilities（IIS 安全漏洞）部分，而不會與 Windows Vulnerabilities 部分那些特定於 Windows 的即時修補程式顯示在一起。同理，任何特定於 SQL 的即時修補程式將顯示在掃描報告中的 SQL Vulnerabilities 部分。

問：爲什麼即使在我安裝了掃描結果中標出的即時修補程式後，仍不能從 MBSA 或 HFNetChk 得到正確的即時修補程式報告？

答：Microsoft 發佈的某些即時修補程式中，包含針對掃描工具不易掃描到的某些項的警告和變通辦法，例如 MS99-041，其中並沒有包括修補程式，而只是一個讓用戶修改其系統上某個特定服務的工具。這類安全公告叫做“通知”或“警告”消息。默認情況下，HFNetChk 將顯示這些“通知”和“警告”消息，除非您使用 -s 開關來禁止這些消息。MBSA 默認情況下也將顯示“通知”和“警告”消息，而且在掃描報告中會給它們加黃色 X 標記，表示工具無法確定該安全公告修復是否已得到應用。即使在用戶應用了某一特定的“通知”或“警告”即時修補後，這兩種工具仍會將這些安全公告包括在掃描報告中。有關“通知”消息的更多資訊，請參見下面這一知識庫文章：http://support.microsoft.com/default.aspx?scid=kb;EN-US;q306460。

問：爲什麼 MBSA 和 Windows Update 報告的結果相互衝突？

答：MBSA 和 Windows Update (WU) 採用不同的方式對系統進行分析。例如，WU 僅包括針對 Windows 作業系統的關鍵修補程式，而 MBSA（和 HFNetChk）可報告 Windows 作業系統和其他 Microsoft 產品（如 SQL Server）缺少的即時修補程式。

此外，有時某些即時修補程式會重新發行，如 MS02-008 和 MS02-009。MBSA 總是確保您在系統上安裝最新的修補程式版本。如果您安裝的是 MS02-008 或

MS02-009 即時修補程式原來的版本，MBSA 將指出此即時修補程式尚未安裝，因爲該修補程式有較新的版本可以提供。而 Windows Update 可能不會指出有較新的版本可以提供，因爲它可能在系統上尋找另一些不同元素來確定此修補程式是否存在。Microsoft 正在解決這種不一致問題，以便 HFNetChk/MBSA 工具、Windows Update、Microsoft Software Update Services 和 SMS 安全修補程式管理都使用同樣的規則來確定一個修補程式在 Windows 系統上是否存在。這樣所有客戶都可以使用最適合他們需要的工具，但仍可以保持結果的一致性。而在目前，我們建議用戶到安全公告上查看他們以前已經安裝、但 MBSA 仍報告說缺少的那些修補程式，以確保他們安裝的確實是最新版本。

問：即將發行的 MS Software Update Services（亦稱 Windows Update Corporate Edition）將如何進行系統和修補程式檢測？

答：MS Software Update Services (SUS) 囊括了已在 Windows Update 上發佈的內容並使用了同樣的用戶端體系結構。所以 SUS 在工作方式上將與現在的 Windows Update 完全一樣。

問：將在 SMS Value Pack 中發行的 SMS 安全工具將如何執行系統和修補程式的檢測？

答：SMS 以 HFNetChk 工具爲基礎來進行系統掃描，然後將結果存儲爲企業報告資料庫，報告哪些桌面和伺服器上缺少關鍵修補程式。SMS 中的資料將與 HFNetChk 和 MBSA 中的資料一致。SMS Value Pack 與 Microsoft 下載中心集成，從而更容易得到必需的修補程式，然後以受控方式將它們直接發送到適當的用戶端。

問：Microsoft 對 MBSA 提供支援嗎？

答：是的，該工具由 Microsoft 支援部門 (PSS) 提供支援。

問：MBSA 將來還會有新的版本嗎？

答：是的，Microsoft 正在計劃改進該工具，使之包括更多功能，如 Windows .Net 伺服器支援、本地化以及更多特定于應用程式的檢查等。

問：我該如何提交對 MBSA 的評論或建議？

答：在下面的位置有一個供用戶進行關於 MBSA 的討論的公衆新聞組：news://microsoft.public.security.baseline_analyzer。或者，用戶也可以通過郵件將評論、問題或建議發送到 mbsafdbk@microsoft.com。